In the Claims

For the convenience of the Examiner, all pending claims are set forth below, whether or not an amendment is made. Please amend the claims as follows:

1. (Currently Amended) A method for detecting decryption of encrypted viral code in a subject file, comprising:

emulating computer executable code in a subject file;

maintaining a list of memory regions that have been read and then modified during the emulation;

flagging a memory area that is read during emulation of a first instruction in the computer executable code;

detecting a modification to the flagged memory area during emulation of a second instruction in the computer executable code;

updating the list of memory regions to include the modified flagged memory ~~area;~~ by:

determining whether the modified flagged memory area overlaps a listed memory region of the listed memory regions; and

if the modified flagged memory area overlaps the listed memory region, updating a dimension of the listed memory region to encompass the modified flagged memory area; and

if the modified flagged memory area does not overlap the listed memory region, adding the modified flagged memory area as a new memory region to the list of memory regions;

determining that one of the listed memory regions is larger than a predetermined size; and

triggering a viral detection alarm in response to determining that one of the listed memory regions is larger than the predetermined size, the viral detection alarm indicating detection of viral code.

2. (Currently Amended) A method of detecting encrypted viral code in a subject file, comprising:

emulating computer executable code in a subject file;

maintaining a list of memory regions that have been read and then modified during the emulation;

determining whether a memory area is read during emulation of a first instruction in the computer executable code and whether the memory area is modified during emulation of a second instruction in the computer executable code;

updating the list of memory regions to include the modified memory ~~area;~~ by:

determining whether the modified memory area overlaps a listed memory region of the listed memory regions; and

if the modified memory area overlaps the listed memory region, updating a dimension of the listed memory region to encompass the modified memory area; and

if the modified memory area does not overlap the listed memory region, adding the modified memory area as a new memory region to the list of memory regions;

determining that one of the listed memory regions is larger than a predetermined size; and

triggering a viral detection alarm in response to determining that one of the listed memory regions is larger than the predetermined size, the viral detection alarm indicating detection of viral code.

3. (Original) The method of claim 2, wherein the emulation is performed on an instruction-by-instruction basis.

4. (Canceled)

5. (Original) The method of claim 2, further comprising:

determining whether a selected one of the listed memory regions is contiguous with the modified memory area; and

updating the selected memory region to encompass the modified memory area.

6. (Canceled)

7. (Currently Amended) A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for detecting decryption of encrypted viral code in a subject file, the method steps comprising:

emulating computer executable code in a subject file;

maintaining a list of memory regions that have been read and then modified during the emulation;

flagging a memory area that is read during emulation of a first instruction in the computer executable code;

detecting a modification to the flagged memory area during emulation of a second instruction in the computer executable code;

updating the list of memory regions to include the modified flagged memory ~~area;~~ by:

determining whether the modified flagged memory area overlaps a listed memory region of the listed memory regions; and

if the modified flagged memory area overlaps the listed memory region, updating a dimension of the listed memory region to encompass the modified flagged memory area; and

if the modified flagged memory area does not overlap the listed memory region, adding the modified flagged memory area as a new memory region to the list of memory regions;

determining that one of the listed memory regions is larger than a predetermined size; and

triggering a viral detection alarm in response to determining that one of the listed memory regions is larger than the predetermined size, the viral detection alarm indicating detection of viral code.

8. (Currently Amended) A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for detecting encrypted viral code in a subject file, the method steps comprising:

emulating computer executable code in a subject file;

maintaining a list of memory regions that have been read and then modified during the emulation;

determining whether a memory area is read during emulation of a first instruction in the computer executable code and whether the memory area is modified during emulation of a second instruction in the computer executable code;

updating the list of memory regions to include the modified memory ~~area;~~ by:

determining whether the modified memory area overlaps a listed memory region of the listed memory regions; and

if the modified memory area overlaps the listed memory region, updating a dimension of the listed memory region to encompass the modified memory area; and

if the modified memory area does not overlap the listed memory region, adding the modified memory area as a new memory region to the list of memory regions;

determining that one of the listed memory regions is larger than a predetermined size; and

triggering a viral detection alarm in response to determining that one of the listed memory regions is larger than the predetermined size, the viral detection alarm indicating detection of viral code.

9. (Currently Amended) A computer system, comprising:

a processor; and

a program storage device readable by the computer system, tangibly embodying a program of instructions executable by the processor to perform method steps for detecting decryption of encrypted viral code in a subject file, the method steps including

emulating computer executable code in a subject file;

maintaining a list of memory regions that have been read and then modified during the emulation;

flagging a memory area that is read during emulation of a first instruction in the computer executable code;

detecting a modification to the flagged memory area during emulation of a second instruction in the computer executable code;

updating the list of memory regions to include the modified flagged memory ~~area;~~ by:

determining whether the modified flagged memory area overlaps a listed memory region of the listed memory regions; and

if the modified flagged memory area overlaps the listed memory region, updating a dimension of the listed memory region to encompass the modified flagged memory area; and

if the modified flagged memory area does not overlap the listed memory region, adding the modified flagged memory area as a new memory region to the list of memory regions;

determining that one of the listed memory regions is larger than a predetermined size; and

triggering a viral detection alarm in response to determining that one of the listed memory regions is larger than the predetermined size, the viral detection alarm indicating detection of viral code.

10. (Currently Amended) A computer system, comprising:

a processor; and

a program storage device readable by the computer system, tangibly embodying a program of instructions executable by the computer system to perform method steps for detecting encrypted viral code, the method steps including

emulating computer executable code in a subject file;

maintaining a list of memory regions that have been read and then modified during the emulation;

determining whether a memory area is read during emulation of a first instruction in the computer executable code and whether the memory area is modified during emulation of a second instruction in the computer executable code;

updating the list of memory regions to include the modified memory ~~area;~~ by:

determining whether the modified memory area overlaps a listed memory region of the listed memory regions; and

if the modified memory area overlaps the listed memory region, updating a dimension of the listed memory region to encompass the modified memory area; and

if the modified memory area does not overlap the listed memory region, adding the modified memory area as a new memory region to the list of memory regions;

determining that one of the listed memory regions is larger than a predetermined size; and

triggering a viral detection alarm in response to determining that one of the listed memory regions is larger than the predetermined size, the viral detection alarm indicating detection of viral code.

11. (Currently Amended) An apparatus for detecting decryption of encrypted viral code in a subject file, comprising:

a code emulator, wherein the code emulator emulates computer executable code in a subject file, and outputs memory access information corresponding to the emulated computer executable code; and

a memory monitor, wherein the memory monitor monitors the memory access information output by the code emulator, maintains a list of memory regions that have been read and then modified during the emulation, flags a memory area that is read during the emulation of a first instruction in the computer executable code, detects a modification to the flagged memory area during emulation of a second instruction in the computer executable code, updates the list of memory regions to include the modified flagged memory ~~area,~~ by:

determining whether the modified flagged memory area overlaps a listed memory region of the listed memory regions; and

if the modified flagged memory area overlaps the listed memory region, updating a dimension of the listed memory region to encompass the modified flagged memory area; and

if the modified flagged memory area does not overlap the listed memory region, adding the modified flagged memory area as a new memory region to the list of memory regions;

the memory monitor further determines that one of the listed memory regions is larger than a predetermined size, and triggers a viral detection alarm in response to determining that one of the listed memory regions is larger than the predetermined size, the viral detection alarm indicating detection of viral code.

12. (Currently Amended) An apparatus for detecting encrypted viral code in a subject file, comprising:

a code emulator, wherein the code emulator emulates computer executable code in a subject file, and outputs memory access information corresponding to the emulated computer executable code; and

a memory monitor, wherein the memory monitor monitors the memory access information output by the code emulator, maintains a list of memory regions that have been read and modified during emulation, determines whether a memory area is read during emulation of a first instruction in the computer executable code and whether the memory area is modified during emulation of a second instruction in the computer executable code, updates the list of memory regions to include the modified memory ~~area,~~ by:

determining whether the modified memory area overlaps a listed memory region of the listed memory regions; and

if the modified memory area overlaps the listed memory region, updating a dimension of the listed memory region to encompass the modified memory area; and

if the modified memory area does not overlap the listed memory region, adding the modified memory area as a new memory region to the list of memory regions;

the memory monitor further determines that one of the listed memory regions is larger than a predetermined size, and triggers a viral detection alarm in response to determining that one of the listed memory regions is larger than the predetermined size, the viral detection alarm indicating detection of viral code.

13. (Original) The apparatus of claim 12, wherein the code emulator performs the emulation on an instruction-by-instruction basis.

14. (Canceled)

15. (Original) The apparatus of claim 12, wherein the memory monitor determines whether a selected one of the listed memory regions is contiguous with the modified memory area, and updates the selected memory region to encompass the modified memory area.

16. (Canceled)

17. (Currently Amended) A medium which embodies instructions executable by a computer for detecting decryption of encrypted viral code in a subject file, comprising:

a first segment, including emulator code, wherein the emulator code emulates computer executable code in a subject file, and outputs memory access information corresponding to the emulated computer executable code; and

a second segment including memory monitor code, wherein the memory monitor code monitors the memory access information output by the code emulator, maintains a list of memory regions that have been read and then modified during the emulation, flags a memory area that is read during the emulation of a first instruction in the computer executable code, detects a modification to the flagged memory area during emulation of a second instruction in the computer executable code, updates the list of memory regions to include the modified flagged memory ~~area,~~ by:

determining whether the modified memory area overlaps a listed memory region of the listed memory regions; and

if the modified memory area overlaps the listed memory region, updating a dimension of the listed memory region to encompass the modified memory area; and

if the modified memory area does not overlap the listed memory region, adding the modified memory area as a new memory region to the list of memory regions;

the memory monitor code further determines that one of the listed memory regions is larger than a predetermined size, and triggers a viral detection alarm in response to determining that one of the listed memory regions is larger than the predetermined size, the viral detection alarm indicating detection of viral code.

18. (Currently Amended) A medium which embodies instructions executable by a computer for detecting encrypted viral code in a subject file, comprising:

a first segment including emulator code, wherein the emulator code emulates computer executable code in a subject file, and outputs memory access information corresponding to the emulated computer executable code; and

a second segment including memory monitor code, wherein the memory monitor code monitors the memory access information output by the code emulator, maintains a list of memory regions that have been read and modified during emulation, determines whether a memory area is read during emulation of a first instruction in the computer executable code and whether the memory area is modified during emulation of a second instruction in the computer executable code, updates the list of memory regions to include the modified memory ~~area,~~ by:

determining whether the modified memory area overlaps a listed memory region of the listed memory regions; and

if the modified memory area overlaps the listed memory region, updating a dimension of the listed memory region to encompass the modified memory area; and

if the modified memory area does not overlap the listed memory region, adding the modified memory area as a new memory region to the list of memory regions;

the memory monitor code further determines that one of the listed memory regions is larger than a predetermined size, and triggers a viral detection alarm in response to determining that one of the listed memory regions is larger than the predetermined size, the viral detection alarm indicating detection of viral code.